

EXHIBIT 1

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

_____	:	
	:	
HEDGEYE RISK MANAGEMENT, LLC,	:	Civil Action No. 1:21-cv-03687-ALC-RWL
	:	
	:	
Plaintiff,	:	
	:	
v.	:	ORAL ARGUMENT REQUESTED
	:	
	:	
DARIUS DALE,	:	
	:	
	:	
Defendant.	:	
	:	
_____	:	

HEDGEYE’S SUBMISSION OF NEWLY OBTAINED EVIDENCE
AND REPLY IN SUPPORT OF RENEWED MOTION
FOR PRELIMINARY INJUNCTION

TABLE OF CONTENTS

	Page(s)
PRELIMINARY STATEMENT	1
I. DEFENDANT’S LATEST AND ONGOING MISAPPROPRIATION	1
A. This Court’s April 27 TRO	1
B. Defendant’s Newly Admitted Contempt	2
C. Defendant Breached His Duty To Conduct A Reasonable And Diligent Search For Documents Responsive To This Court’s TRO.....	3
D. Defendant’s False Representations	4
II. DEFENDANT’S ADMISSIONS CONSTITUTE ACTIONABLE MISAPPROPRIATION AS A MATTER OF LAW	4
A. Defendant’s Source Code Is A Derived File Even If It Contains Changes Or Modifications Rendering It Dissimilar To Hedgeye’s.....	4
B. The Similarity Between Hedgeye’s Subject Files And Defendant’s Source Files Is Irrelevant To This Motion.....	6
C. Defendant’s Argument That He Designed Around The Trade Secrets Proves His Misappropriation.....	8
D. Defendant Ignores His Disclosure To 42 Macro	9
III. HEDGEYE IS ENTITLED TO AN INJUNCTION.....	10
A. Hedgeye Is Entitled To An Injunction, At A Minimum, Against Defendant Accessing The Trade Secrets He Continues To Possess.....	10
B. The Only Reason The Preliminary Injunction Was Denied Has Been Resolved	10
C. Defendant Ignores Multiple Other Bases For Finding Likely Irreparable Harm	10
D. Defendant Ignores That His Misappropriation Of The Customer Lists Independently Creates The Risk Of Irreparable Harm	11
IV. DEFENDANT INTENTIONALLY DESTROYED RELEVANT EVIDENCE.....	12

A.	Defendant Acted In “Bad Faith” Because He Intentionally Deleted The Files And Their Metadata	12
B.	The Deleted Files And Metadata Are Not Otherwise Available	13
C.	The Deleted Files And Metadata Were Relevant	14
V.	THE COURT SHOULD RESOLVE FACTUAL DISPUTES.....	15
A.	The Court Should Weigh The Evidence And Assess Credibility	15
B.	Defendant Is Not Credible	16

PRELIMINARY STATEMENT

Defendant's misdeeds are being uncovered faster than Hedgeye has time to brief them for the Court. *On the day he filed his opposition to Hedgeye's renewed motion, Defendant sent to Hedgeye's counsel in San Francisco a plethora of Hedgeye trade secrets that he had been expressly ordered by this Court to return nearly three months ago.* Defendant continually fails to recognize the gravity of his actions, apparently intent on forcing Hedgeye to bring yet another formal motion for contempt and an injunction ending his continuing access to the trade secrets.¹

Meanwhile, in opposition to Hedgeye's motion, Defendant ignores what he concedes is the black letter law of trade secret misappropriation. His admissions entitle Hedgeye to judgment as a matter of law; meanwhile, overwhelming evidence supports enjoining Defendant from his continuing egregious misappropriation.

I. DEFENDANT'S LATEST AND ONGOING MISAPPROPRIATION

A. This Court's April 27 TRO

Three months ago, this Court ordered *via* TRO that:

- Mr. Dale shall . . . deliver to Hedgeye **any other files that he obtained or created while employed by Hedgeye** that contain Hedgeye trade secrets and/or other confidential information, **all of which shall be referred to herein the "Subject Files"**;
- Mr. Dale shall also deliver to Hedgeye **any and all notebooks** (and copies thereof) that he prepared and/or kept containing Hedgeye trade secrets and other confidential business information;
- Mr. Dale shall deliver to his counsel a copy of **every computer file . . . that includes, was derived from, or represents a modified version of the Subject Files**; these files shall be referred to herein as the **"Derived Files"**;

¹ Hedgeye also has pending with Judge Lehrburger a discovery letter brief regarding Defendant's blanket refusal to answer any interrogatories or produce any documents.

- Mr. Dale shall thereafter preserve and **forebear from accessing or in any way using any and all copies of the Derived Files . . .** in a manner that may be verified in discovery;

Dkt. 13 (emphasis added).

B. Defendant's Newly Admitted Contempt

The day he filed his opposition to Hedgeye's renewed motion, Defendant admitted to further conduct not only constituting misappropriation as a matter of law, but also to having violated virtually every aspect of the Court's TRO order.

Specifically, on Friday, July 23, Hedgeye's counsel in San Francisco received a package² from Defendant's counsel containing **not just one, but two notebooks**, as well as a number of **pictures Defendant had taken on his phone, and emailed to his Gmail account**, of pages of **other notebooks and highly confidential and proprietary Hedgeye trade secrets**. Wallerstein Decl., ¶ 2. Defendant's terse cover letter concedes the documents were produced "[p]ursuant to the Court's [Temporary Restraining] Order dated April 27, 2021." *Id.*, ¶ 3, Ex. A. In other words, they were **produced pursuant to an order issued three months earlier**.

Defendant has not disclosed when or how the notebooks were "found." He has not disclosed when the images were discovered, where they were discovered, or how they were copied to his counsel. Hedgeye knows Defendant took some pictures of Hedgeye trade secrets on his iPhone, and emailed them to his Gmail. But Defendant has not disclosed if or how he searched his phone, or iCloud, or Gmail. Defendant's cover letter purported to identify some documents as "pictures for the period of January, 2017 through March, 2021." *Id.* Hedgeye and the Court are entitled to know how Defendant knows when the pictures were taken, and what

² Hedgeye gives the undeserved benefit of the doubt that it was a typo that Defendant's letter is misdated July 21, and it purports to have been sent "via overnight mail," as the label confirms it was sent on July 22 and scheduled to arrive on July 23.

steps, if any, have been taken to preserve the metadata of the images. These issues must be resolved immediately.

Further, unless he recently spoliated them, Defendant maintains access to these multiple additional trade secret images. Presumably, Defendant maintains copies at least on his phone, in iCloud and/or Gmail. This possibility more than warrants an injunction that, at a minimum, Defendant cease and forebear accessing the images, and permitting Hedgeye to verify the quarantine and removal of the images from Defendant's possession, custody or control.

Defendant's nonchalant production of further smoking gun evidence came with the bizarre caveat that it was "being produced subject to redaction of pages not subject to expedited discovery." Wallerstein Decl., Ex. A. Further, Defendant purports to designate the entire production "Highly Confidential — Attorneys' Eyes Only." *Id.* But the documents are *Hedgeye's* documents, and contain *Hedgeye's* trade secrets. It is Defendant, not Hedgeye, who may not view the confidential information. Defendant's confusion is illustrative of his continuing misunderstanding of Hedgeye's intellectual property rights.

C. Defendant Breached His Duty To Conduct A Reasonable And Diligent Search For Documents Responsive To This Court's TRO

Rule 34 and this Court's precedent makes clear that Defendant's search for documents responsive to the Court's TRO was not reasonable and diligent:

Defendants did little more than manually search one of [the defendant]'s personal email accounts to comply with the Court's Order. That is not enough. Rule 34(a)(1) allows for discovery of documents in a party's "possession, custody, or control," and requires a party "to conduct a reasonable and diligent search for responsive documents."

Mintz Fraade Law Firm, P.C. v. Brady, 2021 WL 621206, at *4 (S.D.N.Y. Feb. 17, 2021)

(quoting *Wilson v. Town of Cheektowaga*, 2021 WL 195348, at *3 (W.D.N.Y. Jan. 20, 2021)).

Defendant does not explain why he was in contempt of the TRO for three months, or why he never corrected his false representations he made to the Court. Even if Defendant was somehow excused from conducting a diligent search in response to the Court's TRO on April 27, he was questioned about the documents at length in his deposition on June 15. *See, e.g.*, Dkt. 65-1 at 188-89. It was **five weeks** after his deposition – July 22, the day he filed his opposition – that Defendant sent to Hedgeye by overnight mail an additional notebook, and dozens of pictures not discussed at Defendant's deposition. Defendant has no excuse for his *per se* contempt.

D. Defendant's False Representations

Defendant's production also proves his prior representations to this Court were false and misleading. For example, Defendant falsely certified that he "fully and in good faith complied with" the production requirements of the Court's TRO. Dkt. 20-1; *see also* Dkt. 28-1 at ¶ 19 ("I have fully complied with the Court's temporary order . . .").

Defendant opposed the preliminary injunction motion by assuring the Court that he had produced everything the Court ordered; that is, all Subject Files, all notebooks, and all Derived Files. Defendant's newest production should be viewed in the context of the frequency and certainty of Defendant's earlier false assurances. *See, e.g.*, Dkt. 36 at 1 ("Mr. Dale is in full compliance having turned over all documents identified and referenced."); Dkt. 36 at 5 ("All [Hedgeye] files have been turned over . . .").

II. DEFENDANT'S ADMISSIONS CONSTITUTE ACTIONABLE MISAPPROPRIATION AS A MATTER OF LAW

A. Defendant's Source Code Is A Derived File Even If It Contains Changes Or Modifications Rendering It Dissimilar To Hedgeye's

Defendant argues that because he made sure his source files are different than Hedgeye's, his misappropriation is not "actionable." Defendant ignores this Court's TRO that defined "Subject Files" as "any [] files that [Defendant] obtained or created while employed by Hedgeye

that contain Hedgeye trade secrets and/or other confidential information,” (Dkt. 13), and “Derived Files” as “every computer file . . . that includes, was derived from, or represents a **modified version** of the Subject Files.” *Id.* (emphasis added). Thus, **Defendant’s source files are “Derived Files” no matter what modifications Defendant made.** And this Court already concluded that Hedgeye’s “derived files, subject files, source codes, and/or formulas would qualify as trade secrets.” Dkt. 51 at 4:7-9.

Defendant’s argument also ignores the overwhelming authority cited by Hedgeye. For example, Defendant ignores the law that even if “defendants’ products **do not actually contain the secrets**, defendants were assisted in their development of their own products by their knowledge of” the trade secrets. *On-Line Techs., Inc. v. Perkins-Elmer Corp.*, 253 F. Supp. 2d 313, 323 (D. Conn. 2003).

Defendant’s opposition ignores the wealth of authority that “information may be improperly ‘used’ in that it is unlawfully acquired and then **built upon or modified** before being disclosed or benefit derived.” *SkinMedica, Inc. v. Histogen, Inc.*, 869 F. Supp. 2d 1176, 1197 (S.D. Cal. 2012). Defendant ignores this Court’s precedent, as well as a vast collection of persuasive authority that in cases like this one, “in which a plaintiff alleges that defendant’s product is derived from plaintiff’s trade secret . . . proof of ‘slavish copying’ is not necessary and an actor is liable ‘for using the trade secret **with independently created improvements or modifications** if the result is substantially derived from the trade secret.’” *Adv. Analytics, Inc. v. Citigroup Glob. Mkts., Inc.*, No. 04 Civ. 3531(LTS)(HBP), 2009 WL 7133660, at *19 (S.D.N.Y. Aug. 5, 2009) (quoting Restatement (Third) of Unfair Competition § 40 cmt. c) (collecting cases); *see also Am. Can Co. v. Manshukhani*, 742 F.2d 314, 328-29 (7th Cir. 1984) (same).

Defendant ignores the law that trade secret cases do not require a “strict comparison” to determine misappropriation. *See BladeRoom Grp. Ltd. v. Facebook, Inc.*, No. 5:15-cv-01370-EJD, 2018 WL 514923, at *9 (N.D. Cal. Jan. 23, 2018). And Defendant ignores the authority that his “**attempt to disclaim use of various elements of the claimed trade secrets** does not foreclose the possibility that [defendant’s] process was substantially derived from the trade secrets, **even if it differed in specifics** from the process described therein.” *Id.*

B. The Similarity Between Hedgeye’s Subject Files And Defendant’s Source Files Is Irrelevant To This Motion

Defendant expressly assumes that to “qualify as a trade secret,” Hedgeye must “identify with particularity a[] specific component common to both companies’ source files that was originally unique and proprietary to Hedgeye” Opp. at 1. He emphasizes that Hedgeye has not yet demonstrated similarity or “commonality” between its Subject Files and Defendant’s source files.³

Again, Defendant ignores the law that he committed actionable misappropriation even if he ultimately used **none** of Hedgeye’s trade secrets. *See On-Line Techs.*, 253 F. Supp. 2d at 323 (Even if “defendants’ products do not actually contain the secrets, defendants were assisted in their development of their own products by their knowledge of” the trade secrets.”).

A defendant commits actionable misappropriation if he uses “negative knowledge” of the trade secret. *Id.* (“[D]efendant’s ‘negative knowledge’ is one form of ‘using’ trade secrets.”). In

³ Hedgeye already has offered expert testimony that Defendant could not have constructed his source files without reference to Hedgeye’s. *See* Dkt. 24. The Court exercised its discretion not to credit that evidence only in light of Defendant’s representations now known to be false. Ultimately Hedgeye will disclose overwhelming expert opinions showing both that Defendant’s source files necessarily derived from Hedgeye’s, and that they do indeed bear too much similarity for Defendant to have created his “from scratch” as he claims.

other words, Defendant is guilty of misappropriation even if the Court credits his testimony that he looked at Hedgeye's trade secrets to ascertain what **not** to include.

Defendant has admitted that he expressly and deliberately changed his own source files based on what he saw in the Hedgeye Subject Files he was using for that purpose. Defendant testified, for example, that he "made sure" that **he would change his own source file** if he saw a particular Hedgeye formula he had in common. Tr. 133:7-12; *see also* Tr. 133:10-12 ("If I did something that inadvertently was in the Hedgeye source file, **I changed my formula.**").

Defendant argues that, "[i]t is one thing to view a source file, but quite another thing to draw upon and employ its content." Opp. at 1; *see also* Opp. at 8 ("Merely opening a file and reviewing its content is far removed from actually incorporating and using the same content in a rival product."). Defendant is right that he describes two different acts; however, **both** acts constitute misappropriation under the law. By making his self-decreed distinction between viewing a trade secret when designing a competing product, on the one hand, and incorporating particular elements, on the other hand, Defendant ignores the law that "[t]here are no technical limitations on the nature of the conduct that constitutes 'use' of a trade secret. . . ."

Restatement (Third) of Unfair Competition § 40 cmt. c.

The parties agree that anything likely to enrich Defendant or harm Hedgeye constitutes use of the trade secret. Opp. at 8. Defendant asserts that "[t]he mere viewing and opening of a file, without more, could not cause harm to Hedgeye, nor enrich 42 Macro in any way." *Id.* But Hedgeye is being harmed, and Defendant enriched, by Defendant using on a daily basis source files he created with reference to Hedgeye's, even if he also modified or changed them.

Finally, Defendant fails to distinguish *Integrated Cash Mgmt. Servs., Inc. v. Digital Transactions, Inc.*, 732 F. Supp. 370 (S.D.N.Y. 1989). It was not because there were certain

similarities or commonalities between the two programs that the court concluded there had been misappropriation. Indeed, the court expressly found that “no direct copying occurred” and that defendants “sincerely attempted to refrain from using ICM source code and other information used by them while working at ICM.” *Id.* at 377. The court entered the injunction because defendants “benefitted from their specific knowledge of the architecture and detail of the ICM programs” in creating their competing programs. *Id.* Here too, Defendant benefitted from the files that he unlawfully copied prior to his departure, even if there was no direct copying.

C. Defendant’s Argument That He Designed Around The Trade Secrets Proves His Misappropriation

Defendant’s insistence that he is not guilty of misappropriation if his resulting files are different from Hedgeye’s rests on a fundamental confusion between different forms of intellectual property. In a patent case, if the accused product does not practice the patented claims – that is, if it is dissimilar enough – then it does not infringe even if the defendant meticulously studied the patent while designing around it. Conversely, if the accused product does read on the claims – that is, if it shares similarity or – then it infringes even if the defendant never viewed the patent.

Trade secrets are the opposite. With trade secrets, it does not matter how similar or dissimilar is the accused product. A defendant may not use a trade secret when designing the accused product, even if the accused product bears no commonality with the trade secret. Conversely, if an accused product was designed without reference to a trade secret, then even an exact replica would be insufficient to find misappropriation. *See, e.g., Prostar Wireless Grp., LLC v. Domino’s Pizza, Inc.*, 815 F. App’x 117, 120 (9th Cir. 2020).

//

//

D. Defendant Ignores His Disclosure To 42 Macro

Defendant concedes that “[m]isappropriation under the DTSA includes the ‘**disclosure or use**’ of a trade secret” *Syntel Sterling Best Shores Mauritius Ltd. v. TriZetto Grp.*, No. 2020 WL 1442915, at *8 (S.D.N.Y. Jan. 27, 2020). Defendant disclosed Hedgeye’s trade secrets to 42 Macro, used them to build his own, and continues to use them daily.

Defendant concedes that “disclosure” is an independent basis for misappropriation, and **entitles Hedgeye to a presumption of irreparable harm**. He then proclaims that he “has not disclosed any trade secrets. He has not disseminated them to others.” Opp. at 2 (citing *Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 118-19 (2d Cir. 2009)).

Defendant’s unsworn *ipse dixit* ignores his sworn testimony that 42 Macro is a distinct, third party entity conceived, established and funded by a third party individual. Mot. at 20-21. Defendant ignores that Mr. Lamar set up and registered 42 Macro LLC, is the managing member and is “the brains behind the operation.” Mot. at 20. Although Defendant claims in media for publicity purposes to be the “founder” of 42 Macro, in reality, he testified that he is but an unpaid employee. *Id.*

Defend misappropriated trade secrets, violating the DTSA and New York law, when he illicitly copied Hedgeye’s files to his Dropbox account. He violated those laws when he copied them to his personal laptop computer. He violated those laws every time he accessed the file, and he violated them every time he chose to include or not include anything based on what was in Hedgeye’s file. And he violates those laws every day as he sells files that are Derived Files as a matter of law and order of the Court.

//

//

//

III. HEDGEYE IS ENTITLED TO AN INJUNCTION

Defendant concedes that “[u]nder the DTSA, an injunction is warranted . . . “to prevent any actual or threatened misappropriation” 18 U.S.C. § 1836(b)(3)(A). Defendant’s misappropriation has been severe, pervasive and ongoing.

A. Hedgeye Is Entitled To An Injunction, At A Minimum, Against Defendant Accessing The Trade Secrets He Continues To Possess

Given Defendant’s July 22 production of a further trove of Hedgeye trade secrets, Hedgeye should at a minimum be granted an injunction against Defendant further accessing Hedgeye trade secrets, whether located on his phone, in iCloud, Gmail, or otherwise.

B. The Only Reason The Preliminary Injunction Was Denied Has Been Resolved

Defendant notes that “[t]he Court found that basic factual issues were subject to significant dispute (‘Mr. Dale states that the formulas he uses to forecast and back-test data are different from Hedgeye’s’).” Opp. at 3. But that factual dispute – whether Defendant’s formulas are or are not different from Hedgeye’s – is not pertinent to this renewed motion.

Defendant correctly recounts this Court’s comment that Hedgeye had not adequately shown Defendant was using the trade secrets, but argues “And it found that ‘plaintiff has not established that it will suffer irreparable harm absent a preliminary injunction.’” Opp. at 3. Defendant’s use of “and” notwithstanding, this Court found that Hedgeye had not established irreparable harm only because it had not proven Defendant’s use of the trade secrets. Mot. at 17.

C. Defendant Ignores Multiple Other Bases For Finding Likely Irreparable Harm

Defendant’s opposition ignores most of the arguments and authority in favor of finding a likelihood of irreparable harm. For example, Defendant ignores that “[e]quitable relief is particularly appropriate in trade secrets cases because ‘loss of trade secrets cannot be measured

in money damages’ and therefore ‘[a] trade secret once lost is ... lost forever.’” *Secured Worldwide LLC v. Kinney*, 2015 WL 1514738, at *11 (S.D.N.Y. Apr. 1, 2015). Defendant ignores his marketing’s “ripple” or “snowball” effect, and its likely concomitant loss of market share. *See Grand River Enter. Six. Nations Ltd. v. Pryor*, 481 F.3d 60, 67 (2d Cir. 2010).

And Defendant ignores *KCG Holdings, Inc. v. Khandekar*, 2020 WL 1189302, at *16 (S.D.N.Y. Mar. 12, 2020); *Lumex, Inc. v. Highsmith*, 919 F. Supp. 624, 631-32 (E.D.N.Y. 1996); *Estee Lauder Cos. v. Batra*, 430 F. Supp. 2d 158, 174, 179 (S.D.N.Y. 2006); and *Spinal Dimensions, Inc. v. Chepenuk*, 16 Misc. 3d 1121(A), 847 N.Y.S.2d 905 (2007). These cases stand for the proposition that “[e]ven where a trade secret has not yet been disclosed, irreparable harm may be found based upon a finding that trade secrets will inevitably be disclosed where, as here, the movant competes directly with the prospective employer and the transient employee possesses highly confidential or technical knowledge” *KCG Holdings*, 2020 WL 1189302, at *16 (quoting *Estee Lauder*, 430 F. Supp. 2d at 174).

D. Defendant Ignores That His Misappropriation Of The Customer Lists Independently Creates The Risk Of Irreparable Harm

Defendant argues that “Hedgeye complains that [Defendant] had a copy of its customer list (which he has since returned) . . . but identifies no instance in which [Defendant] has solicited any of its customers or otherwise used that list in any improper way.” Opp. at 6. But Defendant more than “had a copy of its customer list;” Defendant intentionally and secretly downloaded thousands of names from carefully curated customer lists, trying to disguise his activities by using a false innocuous folder name. Mot. at 22.

And Defendant did not in any way “return” the customer list. First, Defendant has not produced any of the customer lists he misappropriated. Second, even if he did, he would have “copied” not “returned” the electronic files. Defendant consistently refers to “returning”

electronic files but only physical storage media like thumb drives, computers and iPhone may be “returned.” Electronic files may only be copied or deleted. Defendant’s persistent confusion further warrants an injunction against accessing the files he falsely insists have been “returned.”

In any event, Defendant continues to ignore the law that “[i]n general, the imminent use of a trade secret constitutes irreparable harm. This is particularly true when the trade secret is a customer list . . .”). *Gallagher Benefits Servs., Inc. v. De La Torre*, No. C 07-5495 VRW, 2007 WL 4106821, at *5 (N.D. Cal. Nov. 16, 2007).

IV. DEFENDANT INTENTIONALLY DESTROYED RELEVANT EVIDENCE

A. Defendant Acted In “Bad Faith” Because He Intentionally Deleted The Files And Their Metadata

Defendant concedes that he had a duty to preserve the Subject Files and their metadata by March 11, and that he deleted them from his computer long after that, on the day the complaint was filed; *i.e.*, on “April 26. If not sooner.” Tr. 146:16-22.

Defendant argues that Hedgeye failed to “establish that [Defendant] acted in bad faith with the intent to deprive Hedgeye of evidence” Opp. at 10. But Defendant does not dispute that a party acts in “bad faith” whenever evidence is destroyed “intentionally,” or “willfully.” *Passlogix, Inc. v. 2FA Tech., LLC*, 708 F. Supp. 2d 378, 410 (S.D.N.Y. 2010). Defendant disputes that negligence is sufficient to find bad faith but ignores that “[f]ailures to preserve evidence occur along a continuum of fault – ranging from innocence through the degrees of negligence to intentionality.” *Rivera v. Hudson Valley Hosp. Grp., Inc.*, 2019 WL 3955539, at *6 (S.D.N.Y. 2019). Defendant concedes he deleted the files intentionally.

Defendant insists he did not delete the files to deprive Hedgeye of evidence; rather, he did it to protect himself from accusations of misappropriation. But the way he gained that perceived “protection” was to deny Hedgeye the evidence of those files residing on Defendant’s

computer. When a party intentionally acts to delete files that are obviously relevant, and to which there is a duty to preserve, he inherently acts with the requisite intent.

Defendant stubbornly refuses to acknowledge the seriousness of his spoliation, his counsel suggesting only that “he now understands the steps he took were not consistent with best practices or the obligation to preserve all evidence” Opp. at 5. In context, “best practices” is a misplaced euphemism for meeting minimal ethical obligations to the Court and to Hedgeye.

B. The Deleted Files And Metadata Are Not Otherwise Available

Defendant argues that no spoliation occurred because Defendant “maintained copies of all relevant files and produced them in discovery.” Opp. at 2; *see also* Opp. at 10. (“[N]o files have been lost. As [Defendant] explained in his deposition, although he deleted certain files from his laptop, he maintained copies of the same files in his Dropbox”).

Hedgeye need not accept Defendant’s word; Hedgeye was entitled to see if Defendant did indeed maintain copies of all relevant files. Further, even if he maintained copies, Defendant did not maintain the metadata associated with the Subject Files he copied to his computer. This is unlike the situation where the sender of an email deletes it, but the recipient maintains a copy. This is unlike a situation where both the sender and recipient delete the email, but a copy remains on the server. Once a Subject File was copied from Defendant’s Dropbox account to his personal computer, both copies of the files constituted critical evidence independently of one another, even aside from their critically different metadata.

Finally, Defendant argues in a footnote that “it is premature to ask for an adverse inference at this early stage, when it has not been established that any information is irretrievably lost.” Opp. at 11 n. 2. But the Court needs to make preliminary findings now to rule on Hedgeye’s renewed motion.

//

C. The Deleted Files And Metadata Were Relevant

Defendant notes that “[w]ithout any showing regarding the materiality of the evidence, a sanction is not appropriate.” Opp. at 11. But Defendant ignores that those same authorities hold that “[w]hen evidence is destroyed . . . intentionally or willfully[], that fact alone is sufficient to demonstrate relevance.”” *Passlogix*, 708 F. Supp. 2d at 411 (quoting *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 431 (S.D.N.Y. 2004)).

Defendant cannot seriously contest that the deleted Subject Files were relevant. Rather, he suggests that Hedgeye must “establish that any missing metadata would establish misappropriation or even tend to support its claims.” Opp. at 2. This is not the law, for good reason. Because the evidence has been destroyed, Hedgeye likely can never establish what the metadata would have shown. This is the very reason Hedgeye is entitled to an inference; Defendant cannot profit from the lack of evidence he intentionally created.

Defendant does not deny that the metadata, at a minimum, is deleted and no longer available. Courts in New York and elsewhere have explained metadata’s independent evidentiary value, particularly in trade secret cases. “Metadata, frequently referred to as ‘data about data,’ is electronically-stored evidence that describes the ‘history, tracking, or management of an electronic document.’” *Aguilar v. Immigration & Customs Enforcement Div.*, 255 F.R.D. 350, 354 (S.D.N.Y. 2008).

“System metadata reflects

information created by the user or by the organization's information management system. . . . Examples of system metadata include data concerning the author, **date and time of creation**, and **the date a document was modified**. . . . System metadata is relevant . . . if the authenticity of a document is questioned or if establishing who received what information and when is important to the claims or defenses of a party.

Aguilar v. Immigration & Customs Enforcement Div., 255 F.R.D. 350, 354 (S.D.N.Y. 2008) (internal quotation marks and citations omitted) (emphasis added); *see also Kingsway Fin. Servs. v. Pricewaterhouse-Coopers LLP*, 2008 WL 5423316, at *6 (S.D.N.Y. Dec. 31, 2008) (“In general, metadata is relevant when the process by which a document was created is in issue or there are questions concerning a document’s authenticity; metadata may reveal when a document was created, **how many times it was edited**, when it was edited and **the nature of the edits**.”).

Courts in New York and elsewhere routinely issue spoliation sanctions for destruction of metadata. *See, e.g., Dorchester Fin. Holdings Corp. v. Banco BRJ S.A.*, 304 F.R.D. 178, 184 (S.D.N.Y. 2014); *Leidig v. Buzzfeed, Inc.*, 2017 WL 6512353, at *12-13 (S.D.N.Y. Dec. 19, 2017).

V. THE COURT SHOULD RESOLVE FACTUAL DISPUTES

A. The Court Should Weigh The Evidence And Assess Credibility

Hedgeye is entitled to an injunction as a matter of law based on the undisputed facts. To the extent the Court perceives any relevant disputed facts, however, they should be resolved via an evidentiary hearing. *See Fengler v. Nusimatic Americana, Inc.*, 832 F.2d 745, 748 (2d Cir. 1987) (reversing and remanding “with instructions that the district court hold an evidentiary hearing regarding the propriety of injunctive relief”).

“In granting or refusing an interlocutory injunction, the court must . . . state the findings [of fact] and conclusions [of law] that support its action.” Fed. R. Civ. Proc. 52(a)(2). Further, “[i]n making findings of fact . . . a trial judge must assess witness credibility; to determine what is believable and what is not.” *Feng v. Soy Sauce LLC*, 2017 WL 6561160, at *1 (E.D.N.Y. Dec. 22, 2017) (applying Federal Rule of Civil Procedure 52).

//

B. Defendant Is Not Credible

Defendant’s self-stated “purpose in viewing the Hedgeye source files,” (Opp. at 4), has nothing to do with whether he is guilty of misappropriation. Further, in making its findings of fact, Defendant’s self-serving testimony should carry no weight. Defendant argues that, “[a]t his deposition, [Defendant] freely admitted he had viewed Hedgeye source files at various times” Opp. at 3. But this was only after Defendant submitted multiple false statements to the Court, and to Hedgeye, denying that he had accessed the files at all. After being caught copying the files to his Dropbox, Defendant first falsely insisted that he copied the files only “to make sure I had copies of the key models I built in the event HE tried to claim that I was misappropriating their trade secrets” Dkt. 36-1 at ¶ 8.

At each step, Defendant admits only so much as he believes already has been discovered. He admitted to asking a Hedgeye employee for confidential information only after chastising the employee for “ratting me out.” Mot. at 15. Only after Hedgeye informed his then-counsel did Defendant admit to changing his LinkedIn profile to “founder” of 42Macro while he still was employed by Hedgeye. *Id.* at 2. Even then, he falsely denied that the company had been set up, only later admitting at deposition that Mr. Lamar had indeed earlier registered the company. *Id.* at 15.

Defendant copied Hedgeye’s trade secrets to Dropbox hours before resigning, admitting it only after Hedgeye disclosed the results of its forensic examination. Defendant submitted false declarations that he had “returned” the trade secrets, only to recently admit he had neither returned nor reasonably looked for Hedgeye material before making his declarations. Only when confronted at his deposition did Defendant admit to accessing and referring to the Subject Files in designing his own source files. Only when confronted with a picture of a notebook at his

deposition did Defendant suddenly remember to “find” that notebook, as well as some of the images. And of course Defendant deleted the Subject Files, and their associated metadata.

This Court should recognize that Defendant is not credible when it is weighing the evidence and making the findings required on Hedgeye’s renewed motion.

Respectfully submitted,

Dated: July 26, 2021

/s/ Thomas E. Wallerstein

VENABLE LLP

Eric A. Prager

Thomas E. Wallerstein (*pro hac vice*)

1270 Avenue of the Americas, 24th Floor

New York, NY 10020

Tel.: 212-307-5500

EAPrager@Venable.com

TWallerstein@Venable.com

Attorneys for

Hedgeye Risk Management, LLC